WiNG 5.2.6.0-044R Release Notes

Overview

WiNG 5.2.6 is a maintenance release that serves as a release vehicle for the AP 8132 hardware platform.

- AP 8132 - The AP 8132 is a 3-spatial stream access point with two radios, delivering data rates of up to 450 Mbps per radio over WING 5 architecture. The AP 8132 is the industry's first modular access point. Its innovative design lets you simply snap on modules to extend functionality beyond that of traditional access points. With its standard USB interface, the AP 8132 provides virtually unlimited possibilities for supporting a broad range of applications from a wide variety of developers.

Notes:

- WiNG 5.2.6 does not support the NX 4500 & NX 6500 controllers.

1. Platforms Supported

WiNG 5.2.6 supports the following platforms with the corresponding firmware images.

<u>Note: WiNG 5.2.6 is primarily intended as a HW release for the AP 8132, customers not using the AP 8132 are encouraged to use 5.2.13, 5.3.1, or 5.4.0 rather than 5.2.6.</u>

Controller Platform	**Firmware Image**
RFS 4010	RFS4000-5.2.6.0-044R.img
RFS 4011	RFS4000-5.2.6.0-044R.img
RFS 6000	RFS6000-5.2.6.0-044R.img
RFS 7000	RFS7000-5.2.6.0-044R.img
NX 9000	NX9000-5.2.6.0-044R.img
NX 9500	NX9000-5.2.6.0-044R.img
AP Platforms	**Firmware Image**
Dependent APs	
AP 300	Not Supported in 5.2.6.
AP 621	Not Supported in 5.2.6.
AP 622	Not Supported in 5.2.6.
AP 650	Not Supported in 5.2.6.

Independent /Adaptive APs	
AP 6511	Not Supported in 5.2.6.
AP 6521	Not Supported in 5.2.6.
AP 6522	Not Supported in 5.2.6.
AP 6532	Not Supported in 5.2.6.
AP 7131	Not Supported in 5.2.6.
AP 7161	Not Supported in 5.2.6.
AP 8132	AP8132-5. 2.6.0-044R.img

2. New Features in WiNG v5.2.6

WiNG 5.2.6 adds support for the AP 8132 access point platform including 3x3 MIMO operation and data rates.

WiNG 5.2.6 provides no additional fixes or SW features for WiNG over what was introduced in 5.2.12.

3. Controller Licensing in WiNG v5.2.6

This is unchanged from release v5.2.1. It is repeated here for convenience.

Maximum Capacities of license types per controller platform	**RFS4010**	**RFS 4011**	**RFS 6000**	**RFS 7000**	**NX 9000/ NX 9500**
Adaptive AP Licenses applicable to: • AP 8132	36	36	256	1024	10,240 • Appliance will ship with Zero ports

Please note that that AP 300 continues to follow the AP license type and the AP license capacity. It is only supported by the RFS controllers.

4. Firmware upgrade – Controllers and Dependent APs

Note: WiNG 5.2.6 is primarily intended as a HW release for the AP 8132, customers not using the AP 8132 are encouraged to use 5.2.13, 5.3.1, or 5.4.0 rather than 5.2.6.

Please note that upgrading WiNG v4.x networks to WiNG v5.2.6 will not retain the 4.x configuration. Please use the configuration migration utility to convert a 4.x configuration to a 5.2.6 based configuration.

- Adaptive APs deployed in WiNG v4.x will retain their static IPs upon upgrade
- Controller will retain their WiNG v4.x IPs upon upgrade to 5.2.6 (unlike 5.1). Basic network and port settings that are needed to establish connectivity with the switch will be retained as well, when an WiNG v4.x controller is upgraded to WiNG v5.2.6
- An offline configuration migration utility is also available as a win32 executable. The required input is a 'device generated' WiNG 4x configuration file (running-config). The output is a WiNG 5x configuration file. Please use this file as a base for your desired WiNG 5 config. Note that some functionality is not migrated – in particular, see Important Note 1.
- Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Please allow time for devices to complete the upgrade. APs connected directly to RFS 4000 and RFS 6000 controllers need the controller to stay active until the upgrade completes.
- Both the controller and the AP should be upgraded to the same versions – a firmware mismatch can cause network disruptions and should be avoided. When upgrading, the controllers should be upgraded first and then the APs. When downgrading, the APs should be downgraded first, and then the controller.
- Note: There are several changes/fixes done to SMART-RF in WiNG v 5.2 release. If upgrading to v 5.2.6 from a version prior to 5.2, execute the following commands to ensure proper SMART-RF function:
    - service smart-rf clear-config
    - service smart-rf clear-config on rf-domain
    - service smart-rf clear-history
    - service smart-rf clear-history on rf-domain.

Notes:

- Please ensure that the controller and AP are on the same WiNG version after the upgrade is complete.
- Please be aware of the following when upgrading an AP 300 from prior images to WiNG v5.2 with an RFS controller.

4.1 Upgrade/ Downgrade Process for RFS Controllers

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

4.1.1 Upgrade from WiNG v5.x to WiNG v5.2.6

1. Copy the RFSX000-5.2.6.0-044R.img to your tftp/ftp server.

2. Use the ―**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**‖, or ―**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the controller. From CLI the command is ―reload.

4.1.2 Upgrade from WiNG v4.3.x to WiNG v5.2.6

1. Copy the RFSX000-5.2.6.0-044R.img to your tftp/ftp server.

2. Use the ―**upgrade ftp://<ip address of server>/<name of file>**‖ command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the controller. From CLI the command is ―reload.

***Note*:**

- When upgrading from WiNG v4.x to WiNG v5 system, the configuration is not retained or converted. Please use the configuration migration tool to convert a 4.x configuration to a 5.2.6 configuration.
- Please use ftp to upgrade to WiNG v5.4.0 on an RFS 6000, and not tftp, if using GE1.
- **Please note:** due to hardware refresh changes on controllers RFS7000, RFS6000 and RFS40XX, downgrade/upgrade to version that doesn't support new hardware components will be prevented. Following currently released version don't support new hardware: v5.0.x, v5.1.x. v5.2.0, v5.2.1, v5.2.2, v5.2.11, v5.2.3, v5.3.0, all versions prior to v4.4.1.

4.1.3 Downgrade to a WiNG v4.3.X.from WiNG v5.2.6

1. Copy the RFSX000-4.3.X.X-X43R.img to your tftp/ftp server.

2. Use the ―**upgrade ftp://<ip address of server>/<name of file>**‖ command from CLI or **Operations>Device Detail>Load Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the Controller. From CLI the command is ―reload.

Please note: due to hardware refresh changes on controllers RFS7000, RFS6000 and RFS40XX, downgrade/upgrade to version that doesn't support new hardware components will be prevented. Following currently released version don't support new hardware: v5.0.x, v5.1.x. v5.2.0, v5.2.1, v5.2.2, v5.2.11, v5.2.3, v5.3.0, all versions prior to v4.4.1.

4.1.4 Configuration Restoration

On upgrade from 4.x to 5.x the 5.x controller will save the configuration from 4.x in another file on flash (so that 'startup-config' will point to the 5.x default startup-config). The configuration file from 4.x is renamed to startup-config-wing4. The password encryption file is also moved to /etc2/encrypt-passwd-wing4.

On downgrade from 5.x to 4.x the controller will save the 5.x configuration and it is moved to hidden files of the same name (/etc2/.encrypt-passwd-wing5 and /etc2/nvram/.startup-config-wing5). Any previously saved wing4 config if present (ie. startup-config-wing4) is restored back.

4.2 AutoInstall

Auto Install in v5.2.6 works via the DHCP server. This requires the definition of a Motorola Vendor Class and three sub-options that can be either sent seperately, or under option 43:

Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to entered as a string: —ftp://admin:motorola@192.168.1.10‖)

Option 187 - defines the firmware path and file name

Option 188 - defines the config path and file name

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the vlan interface which is being used to perform the above autoinstall.

DHCP vendor class for platforms is noted below:

- MotorolaRFS.RFS4000
- MotorolaRFS.RFS7000
- MotorolaRFS.RFS6000
- MotorolaNX.NX9000
- MotorolaAP.AP8132

5. Firmware Upgrade & Downgrade – Independent Access Points

Note: WiNG 5.2.6 is primarily intended as a HW release for the AP 8132, customers not using the AP 8132 are encouraged to use 5.2.13, 5.3.1, or 5.4.0 rather than 5.2.6.

As AP8132 is a new product, there is no upgrade and downgrade possible at this time.

6. Important Notes

Important notes for AP8132:

1. If using 2x2 mode of operation, antenna ports labeled A and B should be used.
2. “enforce version” should be set to default value when upgrading from 5.2.3-40R
3. Transmit Beamforming is not officially supported although it is mentioned in the GUI & CLI.
4. Extended VLANs are not recommended for use in 5.2.6 with AP 8132.
5. Virtual Controller functionality is DEMO only for AP8132

Note: WiNG 5.2.6 is primarily intended as a HW release for the AP 8132, customers not using the AP 8132 are encouraged to use 5.2.13, 5.3.1, or 5.4.0 rather than 5.2.6.

The following release notes were previously documented in WiNG v5.2.12 Release.

1. WirelessController Access protocols
   - HTTPS/SSHv2/SNMP enabled by default
   - HTTP/Telnet Disabled is by default

2. Only two (2) controllers in a cluster are supported in WiNG 5.2, the same as in WiNG v5.1.x. Cluster creation has changed in WiNG v5.2 as compared to WiNG v5.1.x To create a cluster in WiNG v5.2, please do the following:
   a. Controller 1 needs to be fully configured and functional
   b. For controller 2 to be added:
      - Login to Controller 1. Configure “cluster name” if not already configured.
      - Log in to Controller 2, setup an SVI with a static IP address and make sure you can ping Controller 1 IP address. DHCP is not recommended for clustering since the IP address may change later on and the cluster may not form.
      - From Controller 2, execute “join-cluster <Controller 1 IP> username “admin” and the admins’ password

```
rfs4000-22A3DE#cluster-join 10.10.1.1 username “admin” password “7otorola”
Joining cluster at 10.10.1.1… Done
Please execute “write memory” to save cluster configuration.
rfs4000-22A3DE#
```

The requirement that user has to know the admin user name and pass word of Controller 1 makes sure that only the admin can add new controllers to the cluster. To make sure cluster config persists across reboots, user should do “write mem” explicitly after cluster is formed. The command “joincluster” changes only running-config, not startup-config.

3. Maximum number of clients per AP platform is as follows:

AP Platforms	Client Association Capacities
Dependent Aps	
AP8132	256

The client association capacities are the same per radio/per AP.

4. Maximum number of WLANs supported per Platform

Controller Platform	**WLAN capacity**
NX 9000	1000
NX 9500	1000
RFS 7000	256
RFS 6000	32
RFS 4010/4011	24

5. When using Juniper **ex2200-24p-4g** or related models when connecting Motorola Access Points –disable IGMP snooping on the Juniper switches to ensureAP adoption

6. If using an 802.3af 10/100 power injector to power up the 802.11n APs, when plugged into a Gig E wired switch, please set link speed to 100 full, or user a GigE Power Injector.

7. Important Default Configuration Changes from 4.x to 5.x on the RFS

Description	4.x	5.x
ME1 default IP address	10.1.1.100	192.168.0.1
Auto upgrade enabled	On	On for all other platforms – controllers and AP. Disabled for the NX 9000 by default
HTTP enabled	On	Off
Default User Name/Password	admin/superuser	admin/motorola

8. APs have a shadow or secondary IP for gaining access to the AP if the IP address of the AP is not known but the MAC address is known. To derive the shadow IP address of an AP, use the last two hex bytes of the AP's MAC address to determine the last two octets of the IP address.

   AP MAC address - 00:C0:23:00:F0:0A
   AP IP address equivalent – 169.254.240.10

   To derive the AP's IP address using its factory assigned MAC address

   a) Open the Windows calculator by selecting Start>All Programs>Accessories>Calculator. This menu path may vary slightly depending on your version of Windows.
   b) With the Calculator displayed, selct View>Scientific. Select the Hex radio button.
   c) Enter a hex byte of the AP's MAD address. For example, F0.
   d) Select the Dec radio button. The calculator converts the F0 to 240.
   e) Repeat this process for the last AP MAC address octet.

9. Default mode for a WLAN is tunnel. For Local bridging, please change config to "local bridging".

10. TACACS+ for admin authentication/authorization and accounting is available only on the following platforms:
    a. AP 8132
    b. RFS 7000 / RFS 6000
    c. NX 9000 / NX 9500

11. **AP 300 not officially supported in this release**

12. DFS - Please see new notes in 5.4 – Note 3 above:

13. AP adoption: APs are adopted based on valid SKUs, once discovered under the Autoprovisioning policy. AP's with mismatched SKU still get adopted to the controller, but their radio does not turn on.
14. If the system flash is full from eitherpacket traces, crashfiles or ap-images, then there may not be enough space left on the device to create hotspot pages. If this happens, users must clear enough space from flash to allow hotspot pages to be created.

15. Radius authentication of management users uses a different configuration model from 5.0. So if upgrading from 5.0 to 5.3 and you are using radius authentication for management access, you need to either change it to local authentication before upgrade, or make the mode 'fallback' and then reconfigure after upgrade using the new config model (configuring under aaa-policy).

16. Client load balancing makes decisions based on the average load in a band, in a channel within a band and average AP load. Client load balancing ignores differences in what wlans APs are beaconing. Running client-load-balancing amongst APs with different wlan config, will lead to decisions that may cause clients to NOT associate on a certain wlan

17. Install wizard is available only on the RFS 40XX, among the controller platforms.

18. In WiNG 5.x, antenna power table for the AP 650 has been updated. User should confirm power settings for the AP 650s. In 5.3, the power table for AP 6521 has been updated.

19. Multicipher support: Some of clients keep on sending deauth when associated to wep security wlan in multicipher configuration. Please use different BSSIDs with the same WLAN, with different ciphers.

20. Commit is not allowed with radio config having two wlans mapped with different data rates, as this is not a supported configuration.

21. Air Defense sensor capabilities are supported on all the 802.11n APs in this release, and are available for enabling the WIPS functionality as well as the Network Assurance Capabilities. There are some caveats on managing the AP directly via ADSP, for certain AP platforms:

Network Assurance Toolset when Radio is dedicated as a sensor	**AP 8132**
Spectrum Analysis	Yes
Advanced Spectrum Analysis	Yes
Live RF	Yes
Live View	Yes
AP Testing	Yes
Connectivity Testing	Yes

22. Radio Share functionality (allows for enabling the Network Assurance toolkit in ADSP, without dedicating a radio as a sensor) is available on all the 802.11n APs with some caveats – please see details below:

Network Assurance Toolset with Radio Share	**AP 8132**
Spectrum Analysis	Yes
Advanced Spectrum Analysis	Yes
Live RF	Yes
Live View	Yes
AP Testing	Yes
Connectivity Testing	Yes

25. Built-in RADIUS server is not available on AP 6521.
26. If using TFTP to upgrade an AP 6521, AP 6511 or AP 621, on the TFTP server please configure the following settings:
    a. Per packet timeout in seconds: 15
    b. Maximum retries: 20
27. When using IPODs as clients, you may see WPA2 group key rotation handshake failures while MUs are idle (2.4GHz band). Change the handshake timeout to 2 sec to correct this problem.

From the wlan config, the cli command is: wpa-wpa2 handshake timeout X (where X is the timeout in ms, within a range of 10-5000)

28. Auto assign sensor is not available for AP 6511, AP 6521, AP 621 – since this feature requires a reboot on low memory devices, which cannot be done with Smart RF enabled.
29. For IGMP Snooping version v2, v3, source specific multicast is not supported, this will be addressed in a future release.
30. To safeguard against unknown attacks, it is recommended that management access be restricted to authorized hosts/ subnets. This can be done using the restrict-mgmt-access host/subnet cli command under management-policy.

RFS 7000:

Compact flash card will not work on pre-Rev F RFS 7000 hardware.

NX 9000/ NX 9500:

- NX 9000 requires a laptop with a minimum of 4GB RAM for viewing GUI with greater than 3000 AP.
- Extended VLANs are not supported on the NX 9000/ NX 9500. Only Local VLANs are supported.
- There is no VPN, or Advanced WIPS support on the NX 9000/ NX 9500.

AP 7131: PoE & Gigabit Ethernet Ports

The AP-7131 family features upgraded Gigabit Ethernet (GE) ports. These ports are labeled as follows:

- GE1/ PoE: GE1 is the LAN Port and supports 802.3af, 802.3at (draft) PoE.
- GE2: GE2 is the WAN port.

Single radio models can operate fully with 802.3af power sources. Dual radio models and tri-radio models can also power up two radios and GE1 interface with 802.3af power sources. At higher power levels, 2 radios and both Ethernet interfaces are fully functional in the dual and tri-radio models. Single, dual and tri- radio models can also operate using an A/C power supply. The third radio (dedicated WIPS sensor radio or a future modular off-the-shelf 3G WAN Express Card) on the tri-radio model requires 802.3at power levels, A/C power supply or a Gigabit Ethernet PoE+ injector.

The following table shows the radio and LAN resources available under various power configuration modes for the AP 7131 family:

Available Power	**Radio Resources**	**Ethernet Port Configuration**
Power Status: 3af (12.95W)	2 Radios	GE1 10/100/1000
Power Status: 3at (24W)	3 Radios (Express Card option supported with radios at lower power)	GE1 10/100/1000 GE2 10/100/1000
Power Status: Full Power (30W)	3 Radios (with Express Card)	GE1 10/100/1000 GE2 10/100/1000

When a Motorola 802.3af power injector (AP-PSBIAS-1P2-AFR) is used with AP- 7131 or AP-7131N, then the GE1 or LAN1 port will be limited to 10/100 Mbps. Motorola recommends the 802.3at (Draft) power injector (AP-PSBIAS-1P3-AFR) to be used with AP-7131/AP-7131N configurations.

7. Issues Fixed in WiNG v5.2.6

No outstanding SPRs/CQs have been resolved in WiNG v5.2.6.

SPR/CQ	Description